

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA

v.

YANNICK A. MINANG,

Defendant

)
)
)
)
)
)
)
)
)
)

Criminal No. 17-10376-FDS

OPPOSITION TO MOTION TO SUPPRESS

The United States respectfully submits that the Court should deny defendant YANNICK MINANG's ("MINANG") motion to suppress without the need of an evidentiary hearing. First, the affidavit in support of the search warrant established probable cause that MINANG had committed money laundering offenses. Second, based on the nature of the offense, including the use of particular entities to launder fraud proceeds each associated with Defendant, there was an adequate nexus to the MINANG's residence. Third, the warrant provided a particularized description of the items to be seized and was not overbroad. Fourth, MINANG is not entitled to a *Franks* hearing because there were no inaccuracies in the affidavit.

FACTUAL SUMMARY

On September 28, 2017, FBI Special Agent Kevin McCusker submitted an affidavit to U.S. Magistrate M. Page Kelly in support of a criminal complaint charging

MINANG with concealment money laundering in violation of 18 U.S.C.

§ 1956(a)(1)(B)(i-ii) [Exhibit A]¹ and obtained a warrant for his arrest on the complaint.

The FBI arrested MINANG and his residence (800 West Street, Apt. 1417, Braintree, Massachusetts, the Target Location of the search warrant) on September 29, 2017 at approximately 6:05 a.m. While taking MINANG into custody, in plain-view, FBI agents observed that MINANG had two cellular phones and laptop computer in his bedroom [Exhibit B].² The FBI incorporated these observations and the facts alleged in the criminal complaint into an application for a search warrant that Judge Kelly authorized the same day at approximately 11:04 a.m. [Exhibit C].³ In sum, the two affidavits alleged the following facts:

A. Background of Investigation

The investigation into MINANG began with a bank account in Massachusetts under the name Eunice Offre (“Offre”). [Exhibit A ¶¶ 6-8, 13]. The FBI investigation was part of an ongoing operation looking into a fraudulent scheme known as “Business Email Compromise” (“BEC”). The investigation, targeted not only the participants of the

¹Exhibit A refers to the criminal complaint in this case filed on September 28, 2017 (Docket Entry No. 1).

²Exhibit B refers to an FBI 302 Report regarding arrest of MINANG on September 29, 2017.

³Exhibit C refers to the affidavit in support of the search warrant for the Target Location, which incorporated by reference on affidavit in support of the criminal complaint (Exhibit A).

BEC scheme that “spoofed” and hacked email accounts to defraud victims, but also the participants involved in the laundering of fraud proceeds through bank accounts. *Id.* ¶ 4.

B. August 14, 2017 Transfer of \$172,000 to the Offre Trading Account

In August 2017, the email account of a real estate broker representing a victim in Canada was hacked and used to deceive the victim into wiring money for a real estate closing to an account at Bank of America (“BOA”) in Massachusetts ending in 2565 in the name of “Offre Trading” (the “Offre Trading Account”). On August 14, 2017, under the mistaken believe the funds were going to be used to buy real estate, the victim executed two wire transfers of \$86,000 each to the Offre Trading Account. *Id.* ¶¶ 6-7. The victim reported the fraud to BOA on September 19, 2017, and BOA, in turn, contacted the FBI in Boston. *Id.* ¶ 6.

The FBI obtained records from BOA and learned that Offre had opened the account on August 11, 2017, just two-weeks before the fraudulent transfer. *Id.* ¶ 7. The records also demonstrated that the money the victim wired to the Offre Trading Account - a total of \$172,000 - did not stay there long.⁴ Between August 25, 2017 and August 28, 2017, \$71,000 (now the proceeds of fraud)⁵ was wired to an account in South Africa and

⁴The use of a third party’s account as a kind of “pass-through” account is indicative of concealment money laundering. *See United States v. Hall*, 434 F.3d 42, 53 (1st Cir. 2006) (“[Defendant’s] use of his sister’s name in purchasing the money order is evidence of his intent to conceal because it indicates that he was attempting to disguise the source of the proceeds by having it pass through another person’s control”).

⁵Wire fraud is a specified unlawful activity (“SUA”) under 18 U.S.C. § 1956(c)(7) and was completed upon the receipt of the funds into the account. *See e.g., United States v. Foley*, 783 F.3d 7, 16 (1st Cir. 2015) (“The crime of wire fraud was complete upon Foley’s receipt of the mortgage loan funds”).

\$46,000 was withdrawn to fund a cashier's check payable to "Minang Investments."

The cashier's check – in a classic layered transaction⁶ - was negotiated at Santander Bank. *Id.* ¶ 8.

C. July 3, 2017 Transfer of \$272,250 into the Minang Trades Account

While in the midst of investigating the Offre Trading Account, the FBI learned of an earlier but similar BEC fraud that took place in July 2017 involving another account in Massachusetts. *Id.* ¶ 9. This time, the California victim was deceived into wiring \$275,250 to a BOA account in the name of Yannick A. Minang, d/b/a (doing business as) Minang Trades ("the Minang Trades Account," referred to the affidavit as BOA-7413). *Id.*

Similar to the Offre Trading Account, MINANG opened the Minang Trades Account less than *two-weeks* before the illegal June 22, 2017 transfer into his account. *Id.* ¶ 10. Furthermore, after opening the account with a \$100 deposit, the only other account activity was the movement and laundering of fraud proceeds out of the account. *Id.* ¶ 10. After the California victim wired the \$275,250 to the Minang Trades Account on July 3, 2017, between July 3, 2017 and July 6, 2017, MINANG - the only authorized signer on the account - conducted a series of money laundering transactions. *Id.* ¶ 10-11.

First, MINANG wired \$137,500 to an account in South Africa. Second, MINANG used the funds to purchase two cashier's checks, one payable to "Minang

⁶*See e.g., United States v. Charon*, 442 F.3d 881, 885 (5th Cir. 2006) ("asking a third person to purchase a cashier's check and purchasing property with the cashier's check to disguise the criminal proceeds.... constitute[s] 'layering'")

Investments” and a second to “C Tah Cho” (Carlson Cho, who was later identified as MINANG’s roommate at the Target Location). Third, MINANG conducted four different cash withdrawals in a structured manner, in amounts between \$9,000 and \$9,600, just below the \$10,000 federal reporting requirement. *Id.* ¶ 11.

D. September 22, 2017 Consensual Interview of MINANG

The FBI first went to the Target Location, a two-bedroom apartment located at 800 West Street, Unit 1417 in Braintree, on September 19, 2017. [Exhibit C, ¶ 5-6]. At the time, the agents were looking were first looking into the Offre Trading Account and the account holder, Eunice Offre.⁷ A man named Carlson Cho⁸ answered the door. Cho told the agents that Offre in fact did not live at the Target Location. Instead, Cho told the agents that Offre was an acquaintance of his roommate, whom he identified as MINANG, and provided the agents with MINANG’s phone number. *Id.* ¶ 6. In a later interview, Cho also confirmed that MINANG had asked him to cash a \$35,000 check. The check dated September 28, 2017 was made payable to “C.Tah Cho” and as described above was the proceeds of the BEC fraud. Cho further confirmed that after cashing the check, he gave the \$35,000 in cash to MINANG. *Id.* ¶ 8-9.

⁷While not detailed in the affidavit, the FBI went to the Target Location to look for Offre because the Target Location was the address listed on the Offre Trading Account and her Massachusetts Driver’s License.

⁸Unbeknownst to the FBI agents at the time, Cho was the target of a Homeland Security Investigation based in the District of Maryland. On February 8, 2018, federal agents arrested Cho on a criminal complaint and was later added to a superseding indictment on March 12, 2018 charging conspiracy to commit wire fraud and money laundering in criminal case number 17-cr-661-PWG.

The agents called MINANG and arranged to meet him at a Panera Bread restaurant near the Target Location on September 22, 2017. *Id.* ¶ 6. Before conducting the interview, agents also observed a blue BMW parked in a lot near the Target Location that was registered to a woman believed to be MINANG's mother.⁹ During his interview with the agents, Cho described MINANG's vehicle as a blue BMW. *Id.* ¶ 6-7.

As summarized in the complaint affidavit, during the interview, the agents asked MINANG about the \$275,250 that he had received into his Minang Trades Account on July 3, 2017. [Exhibit A ¶ 12].¹⁰ In response, MINANG provided a false and unbelievable explanation: he told the agents that he was expecting a loan of \$40,000 from an individual he referred to as "Alain" but instead received about \$270,000.¹¹ After receiving too much money, "Alain" provided MINANG with instructions about how to return the excess funds that included wiring \$137,500 to an account in South Africa. *Id.* ¶ 12.

⁹The blue BMW, bearing MA registration 1PD-337, was in fact registered to a woman named Janet Minang at MINANG's previous address, 40 Queens Way, Apt. 9, Framingham, MA.

¹⁰In addition to the statements summarized in the affidavit, MINANG also confirmed that while he previously resided in Framingham (at the address on his Massachusetts Driver's License, 40 Queens Way Apt. 9, Framingham, MA) with his mother, that he no longer lived there and instead had moved into the Target Location with his friend Cho. *See* Exhibit D (302 Interview Report of Yannick Minang on 9/22/2017).

¹¹This statements forms the basis of Count Five of the indictment charging a violation of 18 U.S.C. § 1001(a)(2).

When the agents asked MINANG about Offre, he described her as an intermittent girlfriend and told agents that, similar to his situation, Offre had also received \$100,000 into her account as an investment into her business. *Id.* ¶ 13. Finally, in addition to advising MINANG about the importance of telling the truth to federal agents:

the interviewing Agents advised MINANG that the funds that had been sent to his and Offre's accounts were the result of fraud, and by receiving the transfers, he was helping launder the proceeds of illegal activity through his account.

Id. ¶ 14.

The agents further advised MINANG to not conduct any further transactions with the funds in his accounts, and instructed MINANG to contact the agents if he received any additional funds in a similar manner. *Id.*

E. After MINANG's Interview and the FBI's Warnings, September 24, 2017 Transfer of \$30,000 into MINANG's Citizens Bank Account

Unbeknownst to the FBI at the time of their interview with MINANG, on September 21, 2017, another victim in California was deceived into wiring a total of \$150,000 in funds to three different bank accounts under the mistaken belief that the money would be used for a real estate closing. One of the accounts that the California victim was deceived into wiring \$30,000 was an account at Citizens Bank in the name of "Minang Escrows" (the "Minang Escrows Account").

The California victim reported the fraud to the FBI on September 24, 2017, through an online complaint website called "IC3" (the FBI's Internet Crime Complaint website). In the complaint, the California victim identified the recipient bank account as Citizens Bank account number ending in 8048, with an

account name of “Minang Escorws,” and an address of “800 West Street, Braintree, Massachusetts” [*See* Exhibit E].¹² *Id.* ¶ 15.

As part of the fraud, the California victim wired \$30,000 to the Minang Escrows Account on September 22, 2017 (the same day agents interviewed and warned MINANG). *Id.* The next day, on September 23, 2017, according to bank surveillance video images the FBI obtained from Citizens Bank, MINANG went to two different Citizens Bank branches and withdrew a total of \$18,500 from the Minang Escrows account in a structured manner. At approximately 11:41 a.m., MINANG withdrew \$9,000 at a branch in Dedham; at approximately 12:47 p.m., he then withdrew \$9,500 in a branch in West Roxbury. *Id.* ¶¶ 17-18. The bank surveillance images copied and incorporated in the affidavit and clearly depict MINANG and a date of September 23, 2017 [Exhibit G].¹³

F. The FBI Arrests MINANG at the Target Location and Observes Two Cellular Phones and a Laptop Computer in MINANG’s Bedroom in Plain-View.

The FBI obtained a warrant for MINANG’s arrest on September 28, 2017. On September 29, 2017, at approximately 6:00 a.m., FBI agents arrested

¹²Exhibit E is a redacted version of the online IC3 complaint that the California victim (Victim 3 in the indictment) submitted on 9/24/2017, produced in discovery as MINANG-000421. The reference to “800 West Street” is on page 2 and highlighted. It should also be noted that while the victim reported that the victim had wired \$22,500 to the Minang Trades account, bank records actually reflect a transfer of \$30,000. *See* Exhibit F (an excerpt of the Citizens Bank records regarding the \$30,000 wire transfer from Victim 3 to the Minang Trades Account)

¹³*See* Exhibit G (copies of the bank surveillance images with the date and time enlarged).

MINANG at the Target Location. [Exhibit C ¶ 10]. MINANG answered the door and escorted the agents to his bedroom to get additional clothes. Upon entering MINANG's bedroom, FBI SA McCusker observed a laptop computer laying on top of his bed, a smart phone on the bed stand next to the bed, and a second smartphone on the windowsill. *Id.* ¶ 11.

The application for the search warrant in Attachment B sought records that constituted evidence, fruits, and instrumentalities of violation of 18 U.S.C. § 1956(a)(1)(B) (concealment money laundering) including any laptop computer or smartphone. [Exhibit H]¹⁴ The affidavit further specified that the warrant was seeking authorization to search the contents of any computers and smartphones in MINANG's bedroom. [Exhibit C, ¶ 12]. The remainder of paragraph 12 explained in detail several different reasons why business records would be located on computers and smartphones (¶ 12a-e) and why records can remain on such devices for a sustained period of time (¶ 13a-e).

The items of evidence that the FBI seized from the Target Location included copies of bank checks and records for the individuals and business specified in Attachment B; U.S. currency; a Laptop computer and three cellular phones. Among these three cellular phones, the FBI was only able to search one of the cellular phones, a Samsung Galaxy phone model SM-G930P. From the search of this one cellular phone, the FBI retrieved documents and images that the

¹⁴See Exhibit H (Attachment B to the search warrant).

government will seek to introduce at trial. The government conducted a search of the Laptop computer, but does not intend to introduce any evidence from the search of the computer.¹⁵

ARGUMENT

“A warrant application must demonstrate probable cause¹⁶ to believe that (1) a crime has been committed—the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place to be searched—the so-called ‘nexus’ element.” *United States v. Woodbury*, 511 F.3d 93, 97 (1st Cir.2007) (quoting *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir.1999)).

A. The Warrant Application Established Probable Cause that the Crimes of Wire Fraud Had Been Committed and that Defendant Had Committed Money Laundering Offenses

While Defendant concedes that the affidavit established probable cause that a fraudulent scheme was in fact committed, he nonetheless argues that it failed to establish probable cause that *he* committed a crime because there is insufficient evidence that

¹⁵While the government does not intend to introduce anything from the computer, the government would seek to introduce testimony that it did not locate any reports of legitimate transactions or loan agreements that would support MINANG’s statements to agents.

¹⁶Probable cause is present if “the facts and circumstances as to which police have reasonably trustworthy information are sufficient to warrant a person of reasonable caution in the belief that evidence of a crime will be found.” *United States v. Silva*, 742 F.3d 1, 7 (1st Cir. 2014) (quoting *Robinson v. Cook*, 706 F.3d 25, 32 (1st Cir. 2013)).

Defendant participated in the fraudulent hacking or spoofing scheme that generated the illegal proceeds.¹⁷ The argument has no merit.

First, Defendant's argument that affidavit did not present sufficient facts to prove he committed the crime of wire fraud is entirely beside the point. To state the obvious, the complaint did not charge MINANG with wire fraud. Instead, the affidavit in support of the complaint (and the search warrant) alleged that MINANG committed the crime of concealment money laundering - engaging in financial transactions that in fact involved the proceeds of wire fraud, knowing that the money involved in the transaction represented some form of unlawful activity, and knowing that the transaction was designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the illegal proceeds or, alternatively, to avoid a reporting requirement. *See* 18 U.S.C. § 1956(a)(1)(B). For this reason, Defendant's allegation that he had no role in the scheme is vastly overstated. He had a role and a purpose, and that was the movement and laundering of the money after it was stolen.

The evidence of the underlying fraud is of course relevant. To make a money laundering case, the government has to establish that the money involved in MINANG's financial transactions in fact involved the proceeds of wire fraud, a specified unlawful activity or "SUA." The affidavit did that by describing the nature of the Business Email Compromise ("BEC") scheme and summarizing three different examples where victims

¹⁷*See* Defendant's Memo at pg. 5, n. 7 ("Minang does not argue the warrant failed to establish probable cause to believe a crime was committed altogether").

in Canada and California were deceived into wiring money to accounts associated with MINANG. That fact that the affidavit did not allege that MINANG was involved in actually hacking or defrauding is irrelevant. *See e.g., United States v. Richard*, 234 F.3d 763, 769-70 (1st Cir. 2000) (jury could have found defendant knew property was proceeds of SUA committed by another person; therefore, defendant's acquittal on the SUA does not negate knowledge). Nor was the government required to allege each and every fact of the underlying wire fraud (that is, whether in a particular instance was a "spoof" or "hack") to establish that the money MINANG received was SUA proceeds. *See e.g., Illinois v. Gates*, 462 U.S. 213, 231, n. 6 (1983) (there is no requirement that "each and every fact which contributed to his conclusions be spelled out in the complaint") (internal citations and quotations omitted).¹⁸

Second, Defendant's argument that the proof of the knowledge element¹⁹ – that the Defendant knew "that the property involved in the financial transaction represent[ed]

¹⁸For example, Defendant's insinuation that the affidavit contained incomplete facts because a victim was "left unidentified in the affidavit" is simply misleading. *See* Defendant's Memo at 3. The government, as a matter of Department Justice policy and practice, does not publically identify victims for privacy concerns.

¹⁹The statute itself also makes clear "the term 'knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity' means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State, Federal, or foreign law, regardless of whether or not such activity is specified in paragraph (7) [specified unlawful activity]." 18 U.S.C. § 1956(c)(1). *See United States v. Rivera-Rodriguez*, 318 F.3d 268, 271 (1st Cir. 2003) ("defendant is not required to know what type of felony spawned the proceeds but only that some felony did so"); *United States v. Benjamin*, 252 F.3d 1, 7 (1st Cir. 2001) (defendant need only know money is criminally derived; he does not need to know it is SUA proceeds, nor that bank fraud is an SUA).

some form of unlawful activity” – is lacking because he did participate in the actual hacking or spoofing is also wrong. Instead, “it is clear that a defendant may be convicted of money laundering even if she is not a party to, much less convicted of, the specified unlawful activity.” *United States v. Cherry*, 330 F.3d 658, 667 (4th Cir. 2003); *Richard*, 234 F.3d at 769-70.

While it is true that the simple receipt of illegal proceeds, without more, does not amount to a money laundering violation, much more happened here. The affidavit spelled out compelling circumstantial evidence²⁰ of his knowledge and intent through Defendant’s actions. First, the affidavit detailed how MINANG conducted the transactions and how they were consistent with illegal money laundering activities including the layering of transactions through cashier’s checks; the use of a girlfriend’s account; and structured withdrawals of cash at multiple bank branches to avoid reporting requirements. Second, the timing of MINANG’s opening of the Minang Trades Account

²⁰The First Circuit has also routinely upheld the use of circumstantial evidence to show the defendant’s knowledge of the illicit source of the proceeds. *See e.g., United States v. Rivera-Rodriguez*, 318 F.3d 268, 272 (1st Cir. 2003) (structuring large cash transactions and use of third-party name shows knowledge of illegal source of funds). Furthermore, an intent to conceal or disguise may also be inferred from the convoluted nature of the transaction. *See United States v. McGauley*, 279 F.3d 62, 71 (1st Cir. 2002) (closing three bank accounts, depositing funds into new accounts held jointly with parents, and then withdrawing funds from joint account implied an intent to conceal or disguise); *United States v. Morales-Rodriguez*, 467 F.3d 1, 13 (1st Cir. 2006) (monthly secretive transfers of funds between three separate bank accounts was an attempt to conceal the nature, location, source, ownership, and control of proceeds); *United States v. Hurley*, 63 F.3d 1, 11-12 (1st Cir. 1995) (transaction involved “so many deposits and subdividings of funds that laundering was only plausible explanation”); *United States v. Valladares-Quintana*, 187 F.3d 624, 1998 WL 1085780, *6 (1st Cir. 1998) (Table) (that defendant’s delivery of cash was conducted with intent to conceal or disguise evident from his elaborate efforts at secrecy, including use of codes in setting up delivery).

– just two-weeks before the transfer, with no other account activity – is not only highly suspicious but is indicative of an illegal plan to set up an account to quickly launder, in coordination with others, the funds.

Third, in addition to circumstantial evidence, there is also direct evidence. Prior to MINANG’s structured withdrawals of funds on Saturday September 23, 2017, the day before, on Friday, September 22, 2017, two FBI agents interviewed MINANG and warned him about the illegal nature of money that he had moved and warned MINANG not only to not touch the money he already received had but to contact the FBI in the event that he received funds from other unknown sources. Defendant’s argument that he may have misunderstood the command because the agents only told him not to touch “these funds” (i.e., that money already in the account) is a strained and hyper-technical interpretation of a straightforward situation. *See e.g., United States v. Jewell*, 60 F.3d 20, 22 (1st Cir. 1995) (“The affidavit is to be interpreted in a common-sense rather than a hypothetical or hypertechnical manner”) (citing *United States v. Ventresca*, 380 U.S. 102, 109 (1965)). Rather, the fact that Defendant ignored that warning is indicative of his knowledge and intent.

Finally, MINANG false and unbelievable explanation – that a man he knew only has “Alain” loaned him \$40,000, but mistakenly sent him \$270,000 instead and then provided him instructions on how to return the money (which included withdrawing wiring money to South Africa and withdrawing cash) – is further direct evidence that MINANG had something to hide. *See e.g., United States v. Brown*, 366 F.3d 456, 461 (7th Cir. 2004) (Defendant’s “implausible story” combined with the other aspects of his

statement sufficient for probable cause to arrest); *United States v. Edwards*, 632 F.3d 633, 640 (10th Cir. 2001) (Defendant’s implausible, inconsistent explanations of how he came into possession of the money with dye-packs, among other factors, sufficient for probable cause).

Taken together, under the “totality of the circumstances,” there was more than sufficient probable cause to establish that the crimes of wire fraud had taken place and that Defendant had committed money laundering offenses. *See United States v. Zayas-Diaz*, 95 F.3d 105, 111 (1st Cir. 1996) (“Under the ‘probable cause’ standard, the ‘totality of the circumstances’ disclosed in the supporting affidavits must demonstrate ‘a fair probability that contraband or evidence of a crime will be found in a particular place’”) quoting *Illinois v. Gates*, 462 U.S. at 238.

B. The Affidavit Established Probable Cause that Evidence, Fruits, and Instrumentalities of Money Laundering Offenses Would be Found at the Target Location

With regard to the “nexus” element, the task of a magistrate in determining whether probable cause exists is “to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999) quoting *Illinois v. Gates*, 462 U.S. at 238. Put differently, the application must give someone of “reasonable caution” reason to believe that evidence of a crime will be found at the place to be searched. *Texas v. Brown*, 460 U.S. 730, 742 (1983). Defendant argues that affidavit failed to establish such a nexus because “common sense” does not suggest that someone would be records of

their own financial transactions in their own residence, like a cash withdrawal, and because there was no direct link between MINANG's financial transactions and his phone. *See* Defendant's Memo at 8-9. The argument has no merit for the following reasons.

First, the affidavit clearly established, and it appears not to be disputed, that Defendant in fact resided at the Target Location, a two-bedroom apartment with whom he resided with Cho. As detailed in the affidavit, on September 19, 2017, 10-days before the execution of the search warrant, MINANG's roommate, Cho, told the FBI that he lived in the apartment with MINANG. Agents observed MINANG's vehicle in the Target Location's parking lot. Most significantly, the FBI found and arrested MINANG *at the Target Location*. The fact that Defendant had previously lived in Framingham and listed his previous address on the Minang Trades Account at BOA and the Minang Escrows is an immaterial fact. There is no question MINANG was residing at the Target Location. There was no reason to go to Framingham.

Second, Defendant's criminal conduct was not dated or stale, but was instead recent and fresh. Notably, while the conduct began as early as July 2017, MINANG's most recent criminal conduct took place *a week before* the search warrant. MINANG received \$30,000 in fraud proceeds into his Citizens account (Minang Escrows) on September 22, 2017. The next day, on September 23, 2017, MINANG withdrew \$18,500 of the fraud proceeds in structured transactions. The search warrant took place a week later on September 30, 2017.

Third, while it is certainly true that probable cause to arrest does not automatically establish probable cause to search an individual's home, *see e.g., Feliz*, 182 F.3d at 88 (“[W]e do not suggest that, in all criminal cases, there will automatically be probable cause to search a suspect's residence”), the affidavit in this case established that the laundering transactions involved bank accounts in the names of several purported companies, Offre Trading, Minang Trades, and Minang Escrows, each connected to MINANG.

Moreover, while Defendant claims that affidavit contained intentional false information about the address associated with the Minang Escrows Account, Defendant's allegation is actually incorrect. In fact, according to the IC3 report filed with the FBI on September 24, 2017, the address that *the victim* provided as associated with the Minang Trades Account was “800 West Street, Braintree, Massachusetts.” [See Exhibit C, ¶ 15; Exhibit E]. Thus, in addition to the obvious fact opined in the affidavit - that businesses used computers as well smartphones to conduct business, keep track of transactions, and communicate [See Exhibit C ¶12a-e] – there was specific evidence connecting the companies that MINANG used to launder funds to the Target Location including the Offre Trading Account.

Furthermore, because the nature of the offense involved financial transactions and potential communications and coordination across international boundaries to launder fraud money, there was more than a sufficient basis to believe that evidence of these crimes would be located where MINANG slept, kept his clothes, cellphones and a computer. As the First Circuit has made clear, the “nexus between enumerated evidence

of the crime and the place can be inferred from the type of crime, the nature of the items sought, the extent of an opportunity for concealment and normal inferences as to where a criminal would hide evidence of a crime.” *United States v. Flores*, 888 F.3d 537, 548 (1st Cir. 2018) (citing *United States v. Rodrigue*, 560 F.3d 29, 33 (1st Cir. 2009) (quoting *Ribeiro*, 397 F.3d at 49) (internal quotations omitted)).

Here, without any other business address or location, the most logical place where Defendant could have been expected to keep records, evidence, fruits and instrumentalities was his residence. This includes not only records of Offre Trading, Minang Trades, and Minang Escrows, but the absence of records that would suggest that these entities were involved in legitimate commerce. For example, the absence of a loan agreement with “Alian” would be further evidence that MINANG’s statements were indeed false.

What’s more, in contrast to the D.C. Circuit Court of Appeals decision in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017) that Defendant cites, the agents in this case were not simply guessing that MINANG might have electronic devices at the Target Location. While arresting Defendant inside his bedroom, the agents saw a Laptop computer sitting on his bed as well as two smartphones, including one on the nightstand next to his bed. That is observation is compelling and direct evidence that MINANG had constructive possession of and was actively using electronic devices and that, based on the nature of the scheme, would contain evidence of money laundering offenses.

C. The Search Warrant Provided a Particularized and Limited Description of the Items to be Seized

To be sure, a search warrant must particularly describe the things to be seized to avoid wide-ranging exploratory searches. *See e.g., Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Furthermore, a warrant may authorize the seizure of an entire class of items if it is sufficiently particular to establish probable cause to support the seizure of the entire class and a more precise description is not possible. *See Andresen v. Maryland*, 427 U.S. 463, 480 (1976); *United States v. Parker*, 549 F.3d 5, 10 (1st Cir. 2008); *United States v. Morris*, 977 F.2d 677, 680–81 (1st Cir.1992); *United States v. Diaz*, 841 F.2d 1, 4 (1st Cir. 1988).

Here, while there were categories of documents, they were aimed a particular individuals and entities, namely those associated with MINANG and Offre. *See* ¶ I(A). This was a particularized description supported by probable cause because the affidavit described a series of transactions involving each of these entities. Furthermore, because each of these entities were nothing more than shell companies with an unclear business purpose, the agents could not have been expected to provide a more precise or particularized description. *See e.g., United States v. Young*, 745 F.2d 733, 758-760 (2^d Cir. 1984) (warrant authorized entire class of documents “and other evidence of conspiracy” sufficiently particular because agents could not have known the complete scope and manner of the conspiracy).

For this reason, Defendant’s argument that the warrant in this case was an “all-records” warrant that required the government to show a “permeated by fraud” exception

to the warrant requirement is entirely misplaced. *See e.g., United States v. Falon*, 959 F.2d 1143, 1148-49 (1st Cir. 1992). As evidenced in Attachment B to the warrant (Exhibit H), the application did not seek “all records” contained within MINANG’s residence but instead was tailored to specific entities and a relevant time period. *Compare Id.* at 1148 (“when an individual's allegedly fraudulent business activities are centered in his home ... the ‘all records’ doctrine must be applied with caution it would require extraordinary proof to demonstrate that an individual's entire life is consumed by fraud and that *all* records found in the home were subject to seizure”). Furthermore, while the warrant began with description, “All records . . .” the First Circuit “recognized long ago that a warrant's language must be read in context, such that ‘the general’ tail of the search warrant will be construed so as not to defeat the ‘particularity’ of the main body of the warrant.” *United States v. Kuc*, 737 F.3d 129, 133 (1st Cir. 2013) quoting *United States v. Abrams*, 615 F.2d 541, 547 (1st Cir. 1980).

Even if the warrant could be construed as to justify a search of “all records” for a particular entity or individual (notwithstanding the time limitation), the affidavit established that the entities named in Attachment B were directly involved in the laundering of illegal funds. In other words, this is not a case where the government sought all records of an otherwise legitimate business enterprise involved in fraud. Rather, the affidavit established probable cause that the entities and accounts named in the affidavit were set up solely for the purposes of laundering fraud proceeds.

D. Based on the Four-Corners of the Search Warrant, the Affidavit Established a “Substantial Basis” for Probable Cause and Defendant is Not Entitled to a *Franks* Hearing

Where, as here, a defendant challenges a probable cause determination, the reviewing court should simply ensure that the magistrate had a “substantial basis” for concluding that probable cause existed. *Illinois v. Gates*, 462 U.S. at 239; *United States v. Leon*, 468 U.S. at 915. The scope of review, furthermore, is limited and is focused on “the four corners of the affidavit supporting the warrant application[.]” *United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999) (citing *United States v. Khonusavanh*, 113 F.3d 279, 283 n. 1 (1st Cir. 1997)).

To get beyond the four-corners and obtain a *Franks* hearing, a defendant must make two “substantial preliminary showing[s]”: (1) “a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit”; and (2) the “allegedly false statement is necessary to the finding of probable cause.” *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978); *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017). Defendant has done neither.

First, Defendant’s allegations that the warrant contained false or even inaccurate information is simply incorrect. As described above, the affidavit did not intentionally misidentify the address of the Minang Escrows Account. Instead, as indicated in Exhibit E, it was the victim of the fraud in California that identified “800 West Street, Braintree” as being associated with Minang Escrows. While the precise sentence in paragraph 15 did not make this clear, in the context of the remainder of the paragraph (which begins with how a victim reported a fraud online with the FBI), the information is not

misleading or inaccurate. Furthermore, the additional point not included in the affidavit (that bank records reflected MINANG's prior address in Framingham) is also immaterial because MINANG was clearly residing at the Target Location.

Second, Defendant's allegation that the affidavit inaccurately described the date of his structured withdrawals from the Minang Escrows Account is also incorrect. As clearly depicted in Exhibit G, the date MINANG actually went to two different Citizen Bank branches and withdrew cash from the same account clearly reflects a date of September 23, 2017, a Saturday. The fact that the transactions did not clear until the following business day, Monday, September 25, 2017 is immaterial.

Finally, "a magistrate's determination of probable cause should be paid great deference by reviewing courts," *Illinois v. Gates*, 462 U.S. at 236 quoting *Spinelli v. United States*, 393 U.S. 410, 419,(1969)), and "courts should not invalidate the warrant by interpreting the affidavit in a hypertechnical, rather than a commonsense, manner." *United States v. Ventresca*, 380 U.S. 102, 109 (1965); *see also Woodbury*, 511 F.3d at 98 (1st Cir. 2007) (the affidavit should be examined "in a practical, commonsense fashion[.]"(quoting *Feliz*, 182 F.3d at 86). Even in doubtful or marginal cases, reviewing courts should still defer to an issuing magistrate's "probable cause" determination. *See Ventresca*, 380 U.S. at 107; *United States v. Tiem Trinh*, 665 F.3d 1, 10 (1st Cir. 2011); *Rosencranz v. United States*, 356 F.2d 310, 316 (1st Cir. 1997) ("The Supreme Court made it perfectly clear that . . . doubtful cases should be resolved in favor of the warrant"). Here, a commonsense analysis of the affidavit establishes a substantial basis for probable cause.

E. The Good Faith Exception Applies

Even if the Court finds flaws in the affidavit, the Court should not suppress the evidence because the agents were acting in good faith by relying upon a facially valid warrant. *See United States v. Leon*, 468 U.S. 897, 918-21 (1984). When law enforcement agents obtain a search warrant in good faith and act within its scope, there is “nothing to deter[.]” *Id.* at 921. Furthermore, while recklessness can defeat a claim of good faith, small inaccuracies in a warrant affidavit do not invalidate the warrant if those inaccuracies result from good-faith mistakes. *See, e.g., United States v. Capozzi*, 347 F.3d 327, 332-33 (1st Cir. 2003).

CONCLUSION

For the foregoing reasons, the Court should deny Defendant’s YANNICK MINANG’s motion to suppress without the need of an evidentiary hearing.

Respectfully submitted,

ANDREW E. LELLING
United States Attorney

By: /s/ Neil Gallagher
Neil J. Gallagher, Jr.
Assistant U.S. Attorney

Date: August 8, 2018

Certificate of Service

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Neil J. Gallagher, Jr.

Neil J. Gallagher, Jr.